REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed January 12, 2007. Claims 1-19 are pending in the present application. Reconsideration is respectfully requested for at least the reasons presented below.

The specification has been amended to correct inadvertently introduced typographical errors and to update application number and filing date information. Applicants submit that no subject new matter has been added by this amendment to the specification.

35 U.S.C. §102(e) Rejection of Claims 9, 11, and 12

Claims 9, 11, and 12 are rejected under 35 U.S.C. §102(e) as being anticipated by Doyle et al. (U.S. Patent No. 7,134,012, hereinafter "Doyle"). Applicant submits that Doyle does not disclose each feature of the claims.

Embodiments of the present invention, as recited in the claims, are directed to techniques for detecting spoofing of Address Resolution Protocol ("ARP") replies on a computer network. As described in the application specification, ARP is a mechanism for determining the physical address (*e.g.*, MAC address) of a network device when only its logical address (*e.g.*, IP address) is known. (Specification: page 1, lines 17-19). This is useful, for example, if a source device needs to transmit a data packet to a destination device but only knows the logical (rather than physical) address of the destination device. In this scenario, the source device broadcasts an ARP request containing the destination device's logical address over the network. (Specification: page 2, lines 13-20). In response, a device having the logical address identified in the ARP request (*i.e.*, the destination device) sends an ARP reply containing its physical address and logical address (*e.g.*, MAC/IP address pair) to the source device. (Specification: page 2, lines 21-31). The ARP reply is thus sent in response to an ARP request. In this manner, the source device receiving the ARP reply is able to determine the physical address of the destination device in order to transmit the data packet.

As described in the application specification, ARP reply "spoofing" occurs when an attacker sends a forged ARP reply to the source device in response to an ARP request from

the source device. For example, an attacker device may respond to the ARP request by generating an ARP reply that contains the logical address broadcasted in the ARP request and its own physical address, even though the attacker device is not assigned the broadcasted logical address. This spoofed ARP reply will cause the source device to transmit data to the physical address of the attacker device rather than to the physical address of the true destination device. (Specification: page 3, lines 18-27).

Embodiments of the present invention, as recited in the claims, address the foregoing and other such problems by detecting spoofed ARP replies. For example, independent claim 9 specifically recites, in part "analyzing received ATP packets and information in the ARP collector database to determine when a spoofed ***ARP reply*** has been received on a port of the computer network." (Emphasis added). Applicant submits that at least this feature is not disclosed by Doyle.

Doyle is directed to a method of determining "if a packet has a spoofed source Internet Protocol (IP) address," but not spoofing of ARP replies. (Doyle: col. 2, lines 24-25) In other words, Doyle is concerned with determining whether the logical source address of a data packet has been forged. For a received packet, this is accomplished by checking the source IP and MAC addresses contained within the packet against a table of ARP reply entries. For example, as illustrated in Fig. 6 of Doyle, a data packet is received and the source IP (*e.g.*, logical) and MAC (*e.g.*, physical) addresses contained within the packet are obtained (steps 600, 605). An ARP table is then searched to determine if the source MAC address is stored in the table (steps 610, 615). If the source MAC address is found, the source IP address from the packet is compared to the IP address associated with the source MAC address in the table (step 650). If the IP addresses match, the source IP address from the packet is considered to be genuine and the packet is forwarded to its destination (step 645). If the source MAC address is not found in the table (or the IP addresses do not match), the packet is discarded (step 620). Applicant would like to point out that the processing in Doyle for steps 600, 605, 610, 615, 620, 640, 645, and 650 has nothing to do with ARP replies.

Only after a packet is discarded in step 620 in Doyle, is an ARP request (containing the source IP address) broadcast (step 625). Once an ARP reply is received, the

IP/MAC pair contained in the ARP reply is stored in the ARP table (step 635) so that it can be used to validate the source IP addresses of future data packets. Applicant would like to point out here that while Doyle sends out ARP requests in step 625, Doyle does not determine whether the received ARP replies are spoofed.

Applicant submits that detecting spoofed source IP addresses in data packets, as described in Doyle, is completely different from detecting spoofed ARP replies as recited in claim 9. As described above, Doyle determines whether a source IP address for a data packet is spoofed by verifying the source IP/MAC pair from the packet against a table of ARP reply entries. Therefore, Doyle necessarily assumes that the IP/MAC address pair returned in an ARP reply is genuine -- no spoof check of ARP replies is done. If the ARP table contained spoofed information, the method of Doyle would not be able to distinguish between a correct source IP address and a forged source IP address, thereby rendering the method useless. Since Doyle requires that all ARP replies are genuine (*i.e.*, not spoofed), Doyle fails to teach anything about "analyzing received ATP packets and information in the ARP collector database to determine when a spoofed ARP reply has been received on a port of a the computer network" as recited in claim 9. (Emphasis added).

For at least the foregoing reasons, Applicant submits that Doyle does not anticipate or render obvious Applicant's claim 9. Applicant therefore respectfully requests that the rejection with respect to claim 9 be withdrawn.

Claims 11 and 12 depend from claim 9, and are thus allowable for at least a similar rationale as discussed above for the allowability of claim 9, and others.

35 U.S.C. §103(a) Rejection of Claims 1-8, 10, and 13-19

Claims 1-8, 10, and 13-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Doyle in view of Schunk et al. (U.S. Patent No. 6,980,515, hereinafter "Schunk"). Applicant submits that that the claims are patentable over a combination of Doyle and Schunk.

Independent claims 1 and 15 recite features that are substantially similar to claim 9. For example, claim 1 recites in part

generating a data packet, wherein the data packet includes information from the ARP reply, and an identification of the port on which the ARP reply was received;

storing information contained in the data packet in a database of an ARP collector; and

analyzing the information in the database to determine when ARP spoofing occurs. (Applicant's claim 1, in part; emphasis added).

Claim 15 recites in part "wherein the processor is further operable to analyze information in the database and information in a received ATP packet to identify when a spoofed ARP reply has been transmitted by a host." (Emphasis added). As discussed with respect to claim 9, Doyle fails to disclose or suggest anything about determine spoofing of ARP replies.

Further, Applicant submits that the deficiencies of Doyle in this regard are not remedied by Schunk. Schunk is directed to "a multi-tiered network switch allowing tiered access to system resources." (Schunk: Abstract). As best understood, Schunk makes no reference to ARP spoofing in general, let alone the specific concept of analyzing information to determine when ARP reply spoofing occurs as claimed. Accordingly Applicant submits that even if Doyle and Schunk were combined as suggested by the Office Action (although there appears to be no motivation to combine), the resultant combination would not teach or suggest the various features recited in claims 1 and 15.

For at least the foregoing reasons, Doyle and Schunk, considered individually or in combination, do not render obvious Applicant's claims 1 and 15. Applicant therefore respectfully requests that the rejection with respect to claims 1 and 15 be withdrawn.

Claims 2-8, 10, 13, 14, and 16-19 depend from claims 1, 9, and 15 respectively and are thus allowable for at least a similar rationale as discussed above for the allowability of claims 1, 9, and 15, and others.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Sujit B. Kotwal/

Sujit B. Kotwal
Reg. No. 43,336

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
SBK:mg
60964428 v1